Full Title:

Online Shopping Intention in the Context of Data Breach in Online Retail Stores: An Examination of Older and Younger Adults

All authors and their affiliations

Rajarshi Chakraborty

Department of Management Science and Systems, State University of New York at Buffalo, Buffalo, NY, USA

Jaeung Lee

Department of Management Science and Systems, State University of New York at Buffalo, Buffalo, NY, USA

Sharmistha Bagchi-Sen

Department of Geography, State University of New York at Buffalo, Buffalo, NY, USA

Shambhu Upadhyaya

Department of Computer Science and Engineering, State University of New York at Buffalo, Buffalo, NY, USA

H. Raghav Rao (Corresponding Author)

Department of Information Systems and Cybersecurity, University of Texas at San Antonio, San Antonio, TX, USA

Corresponding author. Tel.: +1 210-458-6300; fax: +1 210-458-6305.

Emails:

rc53@buffalo.edu (R. Chakraborty), jaeungle@buffalo.edu (J. Lee), geosbs@buffalo.edu (S. Bagchi-Sen), shambhu@buffalo.edu (S. Upadhyaya) and mgmtrao@gmail.com (H.R. Rao)

**Online Shopping Intention in the Context of Data Breach in Online Retail
Stores: An Examination of Older and Younger Adults**

Abstract

Data breaches through hacking incidents have become a significant phenomenon in the world of online shopping. These breaches can result in loss of personal data belonging to customers. This study builds a research model to examine people's intention to engage in e-commerce in the context of a significant data breach (the Target breach in December 2013). In addition, this paper focuses on the difference in responses regarding post breach online shopping intent among younger adults (below 55 years) and older adults (senior citizens - above 55 years). Our findings show the importance of internal (self) monitoring of bank transactions in reducing the effect of perceptions of severity of data breaches on post breach online shopping intent particularly for senior citizens. The study also demonstrates that perceptions of severity of a hacking incident are significant drivers of perceived online shopping risk for both age groups. Further, perceptions of severity of a hacking incident are significant drivers of post breach online shopping intent but only marginally significant for younger adults. Trusting beliefs in online shopping services and attitude towards e-commerce are significant for the older generation for post breach online shopping intentions and also for younger adults. Gender is significant for seniors while it is not significant for younger adults. The impact of perceived online shopping risk on post breach online shopping is significantly different between the two age groups. The implication of this research lies in informing shopping websites the need to prepare better plans for notifying customers about not only data breaches but their proposed mitigation steps so as to increase trust and reduce perceived risks associated with online shopping.

Keywords: Online shopping, data breach, trust, perceived risk, internal monitoring, age

1. Introduction

Online shopping has been steadily gaining acceptance around the world, especially in the United States (CMO 2014). Online shopping websites have in some instances replaced physical stores (e.g., books and electronics) (Nanji 2013). The rise in online shopping has partially been attributed to the success of secure payment methods through credit and debit cards. According to recent findings (Retailer 2014), these cards account for over 70% of payment methods used for online shopping. In addition to the increasing payment convenience, time-saving has also been a key factor in the adoption of e-commerce (Alreck et al. 2011). Online stores have improved the overall shopping experience by mimicking the amenities of a physical shopping experience in a virtual world (Verhagen et al. 2014). One such example would be saving items in a “shopping cart” and checking out at a later point. This workflow is akin to dropping objects in a physical shopping cart and walking around the store until it is time to check out. This convenience in online shopping experience has reduced the perceived risks towards online shopping that could have been attributed to the lack of physical tangibility (Nepomuceno et al. 2014). While Amazon has been largely at the forefront, several traditional retail chains are now active online. Target, Walmart and BestBuy often experience as much traffic and transactions through their websites as they do through their physical stores (Banjo 2014).

The literature on information systems and marketing is rich with studies about the adoption and success of online shopping (Childers et al. 2002; Lee and Lin 2005; Moshrefjavadi et al. 2012; Soopramanien and Robertson 2007). Most of these studies have examined trust, convenience and privacy as antecedents. Trust and privacy-concerns, in particular, have remained of sustained interest given the ever-evolving risks and attacks associated with online shopping over the years. According to statistics released by the Identity Theft Resource Center (Forbes

Data Breaches and Online Shopping

2014), in the first half of 2014, 381 reported data breaches led to the exposure of over 10 million records of individuals in the United States. This presents significant danger to personal and sensitive data stored in millions of websites. The most danger is faced by websites that allow customers to make transactions. These include shopping websites where hackers are still able to get past sophisticated firewalls and other security software as was the case with Target in 2013 (Times 2014). In addition to the technical challenges, often personnel in charge of the security of these websites fail to take pro-active actions. Customer names, addresses, email addresses, account numbers, and transaction information are often exposed as a result of many of these breaches (Clearinghouse 2012).

Given that online shopping is an integral part of today's economy, it is important to examine how people's attitude towards it is affected by threats to their personal information. In this paper, we have specified the study's context as the Target data breach (Times, 2014). We evaluate the effect of traditionally held notions of trust, security risk and behavior in online shopping (Miyazaki and Fernandez 2001). This paper's contribution is threefold. First, we have incorporated people's internal monitoring to scrutinize artifacts that might be affected by data or other security breaches. We posit that monitoring habits mitigate some of the security concerns and placate fears that may arise in the aftermath of security incidents like the Target and Neiman Marcus data breaches. Second, while purchasing intent has been studied in the field of information systems, it has not been explored in the aftermath of a major data breach incident that is likely to alter intent. Third, the perspective of generational differences has not been examined in prior literature. This paper looks at the difference between two age-based demographics – one below 55 and the other above 55. Traditionally, the latter is referred to as the "senior citizens" generation (older generation) with those between 55 and 60 representing the first tail of it. The reason for this comparative approach is twofold: (1) research has shown significant differences in privacy concerns between older and younger computer users (Goldfarb and Tucker 2012) and (2) testing our hypotheses on a younger sample gives us perspective to interpret the findings from the

Data Breaches and Online Shopping

older population. As our findings will show later in this article, there are significant differences in certain fundamental causality aspects of trust and risk driven behavior on the Internet between these two broad categories of the U.S. population.

To summarize, this paper focuses on the difference in responses regarding post breach online shopping intent among younger adults (below 55 years) and older adults (senior citizens - above 55 years). Findings show the importance of internal (self) monitoring of bank transactions in reducing the effect of perceptions of severity of data breaches on post breach online shopping intent, particularly for senior citizens. The study also demonstrates that perceptions of severity of a hacking incident are significant drivers of perceived online shopping risk for both age groups, and while they are significant drivers of post breach online shopping intent for seniors, they are only marginally significant for younger adults. Trusting beliefs in online shopping services and attitude towards e-commerce are significant for the older generation for post breach online shopping intentions and also for younger adults. Gender and the impact of perceived online shopping risk on post breach online shopping are significantly different between the two age groups.

In the remainder of this paper, we first discuss recent data breaches serving as the background of our study. Then we present the development of our research model. After that the data collection and the analysis are discussed, following which the paper concludes with a focus on the current limitations and the opportunities for future research.

2. Prior Literature

According to a report by the Department of Homeland Security Dark_Reading (2010), 73% (365 respondents out of 500 respondents) answered that they may not purchase merchandise from online websites that have experienced security breaches. Such incidents have triggered customers' protective behaviors such as avoiding using online stores, switching to another online

Data Breaches and Online Shopping

store, and using offline stores (Lee and Lee 2012). Khalifa and Limayem (2003) also found that customers will shop on ecommerce sites more frequently if they do not worry about risks of security breaches.

In addition to online shopping cases, offline business research has also provided similar findings. Belanger et al. (2002) studied the impact of security breaches on hotel revisit intention, likelihood of hotel recommendation and satisfaction. Their results showed that breaches resulted in negative impacts on all outcome variables. This indicates that consumers are highly concerned about data breaches.

Customers' credit card information and other personal information are some of the most commonly stolen items during data breaches into the systems of shopping websites (Peretti 2008; Zeller 2005). Upon a breach and an improper access to such information, these customers become vulnerable to unapproved purchases. Information like mailing address also has the potential of being misused for exploits. Often such exploits can be harder to detect and their effects can be felt by victims in the real world. Online transactions are seldom carried out with complete information about privacy protection from the store owner (Acquisti and Grossklags 2005). On the other hand, customers of online shopping are rarely given the option to choose what information they should provide to the website for the transaction and any additional benefits. For example, storing information about one's favorite local store requires providing one's zip code. Often a transient piece of information for the completion of a transaction may be enough to put a customer at risk after a data breach. Thus, any data breach into these businesses can potentially lead to identity theft.

Baier (1995) defined trust as the "accepted vulnerability to another's possible but not expected ill will toward one" (p. 99). Customers know the kind of risk they are taking, however, the individual customer is often disposed to trust that nothing bad will happen to them. They have positive expectations regarding online shopping websites in their provisioning of shopping services. A fundamental antecedent of technology adoption (Davis 1989) is the decision to trust a

Data Breaches and Online Shopping

technological artifact. Trusting or distrusting of an artifact is based on an individual's general disposition to trust others (McKnight et al. 2002). The Web Trust Model (McKnight et al. (2002) explains the causality of trust on behaviors in the form of decisions made on the Internet. These decisions usually pertain to actions like shopping and sharing information on the Internet. More recently, however, researchers have started to investigate these decisions in the light of both negative and positive beliefs about the potential outcomes (McKnight and Chervany 2001). While most people may trust their frequently visited shopping websites with respect to service quality, repeated stories of breaches may arouse concerns and distrust amongst them. Media reports about breaches can lead to a significant drop in consumers' trust in the security-related capabilities of shopping websites. Whether trust and distrust are distinct constructs or the opposites of a trust–distrust continuum has been debated. Omodei and McLennan (2000) proposed that trust and distrust are two ends of the same scale. Luhmann (1979) posited that while trust and distrust are essentially the same construct, they are distinct functional equivalents. Therefore, in our paper, we considered trust and distrust (as a lack of trust) in the same construct.

Disposition to trust has been constantly changing through generations (Kumar and Lim 2008; Morris and Venkatesh 2000; Sutter and Kocher 2007). For instance, around 1996, Internet through the Web (i.e. the Mosaic Web browser) became mainstream. People at that time who were in their late 30s (i.e. 55 and above at the present time) were the last generation to whom Internet was introduced as a niche technology. Studies about differing perceived usefulness of IT across age groups have shown that the general perception about the Internet is different among people above 55 and those below (Mitzner et al. 2010). According to (Robinson and Jackson 2001), younger Americans are less trusting of fellow human beings than their older counterparts. (Reisenwitz and Iyer 2007) have shown that there is no significant difference between younger baby-boomers and older baby-boomers in terms of most behavioral variables. Also, traditionally, the age of 55 years has been shown to be an important lower bound for studying Internet behavior in the older population (Vuori and Holmlund-Rytönen 2005). The fundamental concepts of trust

Data Breaches and Online Shopping

and risk-taking are the differentiators between younger adults and people over 55. In the context of online shopping, given the importance of security and privacy, awareness about security hazards can also be a significant differentiator. Grimes et al. (2010) have shown that older adults are generally less aware of security hazards on the Internet compared to their younger counterparts. Also, older adults tend to be generally more risk-avoiding than younger adults, regardless of the domain (Roalf et al. 2011). In a similar vein to the above mentioned literature, we take a perspective of generational differences to explore the relationship between risk and trust on online shopping decisions.

Of course, trust is not the sole predictor of online shopping behavior. People may make a risky online purchase without trust or with a low level of trust. For instance, other antecedents such as attitude towards e-commerce may influence customers in their decisions regarding online transactions. According to (Smith et al. 2011), attitude is a function of online stores' privacy policy where the organizations disclose their intentions on how they will use their customers' information. In the e-commerce setting, the level of privacy protection perceived by customers can counteract the negative effect of level of uncertainty in a transaction (Aksoy et al. 2013). For customers, it would be easier to accept and use the electronic distribution channel when level of perceived attitude toward E-commerce site is high.

The lack of transparency, especially in the immediate aftermath of a security breach, often contributes to strains in the relationships between shopping websites and their customers (Grabner-Kraeuter 2002). Customers may discover identity theft and fraud through some irregularities or suspicious transactions in their bank statements, especially if the banks do not use sophisticated fraud detection systems. Other potential signals of fraud may include getting locked out of one's accounts and speculative reports from the news media. If the bank of the affected payment method fails to detect a fraud over a prolonged period after the breach, then it is possible for a customer to feel repercussions through future identity theft incidents. For every kind of potential fraud borne through a data breach, proactive measures to stay alert can help.

Data Breaches and Online Shopping

Internal monitoring is an important element for online shoppers to safeguard themselves against data breach, fraud and identity theft. One of the benefits of e-commerce and online banking is that customers can check their accounts online at any time of the day from any location in the world. This service is usually free of charge and can be an advantage in coping with potential frauds. Checking one's bank statements regularly effectively gives customers a transparency to potential vulnerabilities. According to (Milne 2003) often individuals do not consider tracking the credit report (a form of internal monitoring) as a preventative measure, in part, because of lack of awareness. Since most purchases over internet are done using credit cards, communications programs from retail stores can be an important factor to alert consumers to be watchful of, and monitor their credit records (Piquero et al. 2011).

Thus, we consider monitoring and age demographics to be important issues in the discussion of online decisions that are significantly influenced by trust and risk perceptions. Monitoring is an active form of awareness that, to our knowledge, has typically not been studied in examinations of phenomena about Internet and security and is much more important today since data breaches are commonplace now. On the other hand, information asymmetry can reduce trust and increase perceived risks about online shopping in the current security environment (Miyazaki and Fernandez 2001). In this study we investigate how security threats such as data breaches, in spite of the opportunities to monitor, can potentially impact a person's intention to conduct business with a shopping website.

3. Research Model

A person will have less concern about protecting information that she/he does not deem valuable. Credit/debit cards and other personal information are critical to customers' wellbeing as their misuse can cause material stress. When a shopping store's database or any other internal system is breached, several information nuggets are at risk of being exposed to hacker(s). These

Data Breaches and Online Shopping

often include the username and password and several other personally identifiable information necessary for shopping activities. Most people tend to reuse their passwords across different online properties (Ives et al. 2004). Hence data breaches at a single store can often expose several other online accounts of these customers. Banks today are capable of alerting their customers about suspected security breaches and fraudulent uses of payment cards. In response to such events, retail banks would usually either lock down the account or cancel the payment card. Thus, for the customers, concerns pertain more to the misuse of other information that hackers can get through these data breaches.

Buffett et al. (2004) have shown not all individuals value the same type of information equally. For instance, person A may not treat her cell phone number as a sensitive information as much as person B does. Person A is expected to feel less outraged than person B at an unauthorized sharing of her cell phone number. In other words, not every person should be expected to perceive the same level of severity of the outcome of a data breach. Perceived severity in our study is a proxy for the level of “seriousness” of a security issue at a shopping store, as perceived by an individual. According to (Ng et al. 2009), a user’s perception of severity about these outcomes should lead to behavior that prevents such outcomes from materializing. In the context of our study, that implies stopping or reducing e-commerce transactions with online stores that share characteristics with Target. We thus hypothesize the following:

H1: Perceived severity of security breaches has a negative effect on post-breach shopping intent.

Perceived severity of any kind of data breach in an e-commerce system reduces the likelihood of shopping online. A similar impact is possible on engagement in activities that improve the shopping experience. Such activities include saving payment information on the website. We argue here that such fears can be countered by being proactive about security. This phenomenon is often seen in general Web browsing. People are aware of hackers and their malicious activities exploiting vulnerabilities. However, many of them tend to have that fear reduced by proactively taking steps like installing anti-virus and anti-spyware and often

Data Breaches and Online Shopping

configuring firewalls. We argue there is a parallel between this scenario and the one about shopping. The difference is that anti-virus software blocks a security threat directly while being alert about spending activities is part of a best-effort action to cope with and monitor security threats indirectly. The recent spate of attacks against stores like Target was not directed at specific customers. To cope with the repercussions of these attacks, a specific customer can monitor unusual spending since her payment method(s) may have been exposed to malicious groups of people. This coping mechanism should mitigate the “seriousness” aspect of the attack and affect her desire to shop again. We thus hypothesize the following:

H2: Internal monitoring reduces the impact of perceived severity of security breaches on post-breach shopping intent.

In the context of online shopping, these risks can arise in the context of security, privacy and quality of shopping service. The focus of our study is the consequences of data breaches to customers of online shopping stores. In that context, it is apparent that when a customer will sense a significant risk of an online service being disrupted by malicious people, thus possibly putting her personal information at a risk, she will tend to engage less with such a website. This could be true in spite of her faith in the shopping service-related attributes of the very same website. This concern is magnified when several shopping websites, especially the high-profile ones like Target, face disruptions and breaches. A magnified sense of security risk faced by online stores is thus expected to reduce the desire to pursue online shopping to an even greater degree.

In his classic article, Bauer (1960) mentioned that perceived risk has components of uncertainty - the likelihood of unfavorable outcomes, and consequences - the importance of a loss (Chang and Tseng 2013). This sense of risk is a strong manifestation of the misgivings that a customer has in the security of shopping websites in general, which we operationalize through a construct called Perceived Online Shopping Risk (POSR). POSR stems from the uncertainty of data breach resulting in potential post purchase financial loss through potential violation of

Data Breaches and Online Shopping

private information. Personal or financial information may be stolen from the websites' database by hackers. Consumers may not engage in online shopping, if personal information might be at risk and monetary loss can be a possible outcome (Ling et al. 2010). This reasoning leads us to the following hypothesis:

H3: Perceived online shopping risk has a negative effect on post-breach shopping intent.

In the consumers' mind, perceived severity of security breach manifests itself in the fear of potential consequences of an event. Consumers are afraid of the consequences that may create personal problems for them. Consumers would have negative feelings toward these severities when they know that one of the websites that they regularly visit to shop online has suffered data breaches. For instance, (Miyazaki and Fernandez 2001) found that internet users' top-three concerns with regard to online shopping were privacy loss, system security breaches from third parties (due to faulty technological security), and security breaches that included fraudulent online retailer behavior. Personal information leaks, hackers' intention to harm the consumers, and banking information leak due to the website's breached data storing system were all concerns of consumers.

Survey results cited by (Hoffman et al. 1999) and (Belanger et al. 2002) support that consumers' often cited reasons for rejecting online transactions were their concerns about the lack of information privacy and the potential loss of control over confidential information. Because e-services are based on the continual transmission, processing, and storage of often sensitive financial or personally identifiable information, many consumers may reject using an e-service, due to perceptions of risk (Featherman et al. 2010). A shopper's belief about shopping websites' security vulnerabilities is a strong indicator of inherent cynicism about online security in general. Thus, it is evident that consumers' perception about security beach in a website makes them nervous about all the perceived risks associated with it. This brings us to the following hypothesis:

Data Breaches and Online Shopping

H4: Perceived severity of security breach has a positive impact on perceived online shopping risk

E-commerce involves the primary activity of purchasing products and services through a website by using an electronic payment method like a debit/credit card. In order to engage in this activity, one has to get comfortable with several components that collectively form one's shopping experience. The most important would be the fundamental idea that one can buy something without walking into a store. Engaging in transactions in the virtual world eliminates the opportunity to interact face to face with store employees and to possibly test the product in person. That can create a certain level of discomfort especially in generations that did not grow up with such virtual shopping experiences. In addition to the virtual aspect, payment and personal information are often handled in unprecedented ways. In order to expedite the checkout process most shopping websites give the customers the opportunity to save personal information like name, address, email address and phone number and payment methods like credit or debit card information on the website. For generations that grew up with cash transactions, this is a sometimes an unsettling experience, especially if the entity that is asking for such information does not have a human face to it. We operationalize this comfort-level with some of the key aspects of e-commerce as E-Commerce Attitude (EA). Attitude towards online shopping has previously been shown to be a strong indicator of actual online shopping behavior (Moshrefjavadi et al. 2012). Knowledge about data breaches can reduce the keenness on shopping online or affect the habit of saving important information on websites. However, since attitude is one of the key indicators of behavioral intention in online shopping (Moshrefjavadi et al. 2012), we suggest that a person demonstrating a higher comfort level with most e-commerce attributes will be less likely to be affected. We can thus hypothesize the following:

H5: E-commerce attitude has a positive influence on post-breach shopping intent.

Online shopping-related risks include security risk and privacy risk (Doolin et al. 2005) which decrease the overall utility (benefit) the consumer obtains from shopping on the Internet.

Data Breaches and Online Shopping

The higher the consumer's perception of the risk associated with shopping on the Internet, the higher would be their perception of the variance or uncertainty in the benefits derived. If the consumers think shopping on the Internet is highly risky, they would expect a large variance in the utility from shopping on the Internet (Bhatnagar et al. 2000). Once consumers have learned that online shopping could produce negative consequences, they will avoid those consequences by decreasing online shopping activity (Chiu et al. 2014). Consumers implicitly evaluate the relative worth or importance of benefits against the cost (perceived shopping risk) of e-commerce to form a value assessment. When such value assessment results in a perception of decreased utility, it would have an impact on consumers' attitude toward e-commerce. Therefore, we propose the following relationship:

H6: Perceived online shopping risk has a negative effect on e-commerce attitude.

Trust has been established as a strong predictor of attitude towards many online behaviors, specifically online shopping (Wang and Tseng 2011). With the increased improvement in encryption technology, more shopping sites are offering information storage options for customers both for the purpose of improving their shopping experience and to increase their likelihood of returning. Those who feel most comfortable with these information storage options are deemed to have a more positive attitude towards e-commerce in general. Quality of shopping service, on the other hand, may comprise of the browsing capabilities on the website, the transaction process and finally the matching of the quality of the delivered product or service to that what the customer expected. When a shopping site scores high on all of these quality-related attributes, it is natural for the customer to have a higher trusting belief in that website and the store in general. This positive belief and expectation should naturally increase the comfort level of customers with a specific website as well as online shopping in general. Based on this reasoning, we hypothesize the following:

H7: Trusting belief in shopping services has a positive effect on e-commerce attitude.

Data Breaches and Online Shopping

A consumer's trust in shopping websites can stem from her experience with the overall service being offered by the store even though the website is simply a gateway to it. This trust is often a strong indicator for the return of customers to the website for future purchases. Most of the successful shopping stores that operate both through a website as well as through a physical store have good reputation for conducting their business ethically given the enforceable customer-protecting legal frameworks in play today. With this reality, it is seldom a trend where multiple customers over a prolonged period feel "ripped off" or come out dissatisfied with the service of a shopping store. As for the online version of this experience, customers feel their trust in the service quality is often reduced by the experience of browsing the website and/or from the dissatisfaction with the product bought or the handling of the payment. Often these service quality-related factors compete strongly with security and privacy concerns about the retail outlet for that service, especially since for many people, security or privacy aspects do not completely define the shopping experience. In fact, a website could potentially reduce the quality of the shopping experience by implementing a security or privacy feature that may hinder the workflow of the customers. When a website, that one does not necessarily shop at, gets impacted by a security incident, a consumer is less likely to be affected by security principles. Given that literature (Xu et al. 2005) has shown that trusting beliefs are a major indicator of adoption of technology, we hypothesize the following:

H8: Trusting belief in shopping services has a positive effect on post-breach shopping intent.

The constructs involved in the proposed hypotheses are operationalized by the variables defined in table 1. The following section describes how these variables were measured. The variable relationships taken together explain the underlying social and environmental conditions that "cause" a certain social behavior to happen. The research model is depicted in figure 1.

Table 1: Variables for Research Model

Variable Name	Definition of Variable	Measurement

Data Breaches and Online Shopping

1	Post-Breach Online Shopping (PBOS)	Likelihood of continuing shopping and showing favorability towards a shopping website like Target.com in the light of the data breach at Target.com.	(Hong and Cha 2013)
2	Perceived Severity (PS)	What would be at stake for a person if one of her shopping websites faced a hacking incident.	(Ng et al. 2009)
3	E-Commerce Attitude (EA)	General comfort level with practices and habits commonly associated today with online shopping.	Self-Developed
4	Perceived Online Shopping Risk (POSR)	Perceived risks that shopping websites and online shoppers in general face today.	(Cho 2006)
5	Trusting Beliefs in Shopping Services (TBSS)	Trust that a user may have in the quality of shopping service offered by shopping websites in general	(Lee et al. 2012)
6	Internal Monitoring (MON)	Person's frequency of checking her bank statement(s)	Self-Developed

Figure 1: Research Model

4. Data Collection

The data were collected one month after the massive Target data breach attack that happened in mid-December 2013¹. We created a survey and got IRB permission to launch it. We collected data through an online survey conducted by Qualtrics. Qualtrics found eligible respondents (young adult < 55 and Senior citizen >=55) based on a random sampling of their

¹ <https://corporate.target.com/about/shopping-experience/payment-card-issue-faq>

Data Breaches and Online Shopping

national database and distributed the survey to each group. Specifically, Qualtrics contacted individuals through email announcements in their database that matched our criteria. Each individual respondent could choose the time and place to respond. Moreover, respondents could withdraw from the survey any time without any penalty. As we were interested in differences between below-55 and above-55 (senior citizens) groups of the U.S. population, we conducted two surveys. The sample size from the former was 159 while that from the senior citizens' category was 205. Henceforth in the remainder of this paper, we shall refer to the two datasets as the "younger" and the "senior (or older) citizens" datasets respectively for convenience. For both the samples, we used a filter that screened respondents - they must have shopped online at least once in their life. Not satisfying this filter would have rendered the rest of the survey instrument meaningless and not applicable to this study.

The online survey was utilized to empirically test the research hypotheses presented above. The constructs were measured based on self-reported scores through the online questionnaire. Most of the items used to measure the constructs in the model were borrowed/ or adapted from literature and all variables were measured on a 5-point Likert scale. Items for Perceived Online Shopping Risk (POSR) (Cho 2006) as well as those for Trusting Beliefs in Shopping Services (TBSS) (Lee et al. 2012) were adapted to the context of online shopping. Perceived Severity (PS) was measured by adapting items for online shopping from (Ng et al. 2009). We measured internal monitoring (MON) through two self-developed 5-point Likert scale questions. In order to develop Internal monitoring measurements, we conducted interviews with two information security professionals in a local bank. Based on the interviews, we created two measurements. 1) I sign up for spending alerts for all my payment cards 2) I track the charges on my bank statement. However, only one of them turned out to load significantly both in Factor Analysis and PLS (described later). The significantly loading item for MON measured the frequency of checking one's bank statements, which was used as a proxy for wanting to stay aware of misuse of credit or debit cards. The dependent variable, Post-Breach Online Shopping

Data Breaches and Online Shopping

(PBOS) intent measured intent of continuing online shopping activities as usual, by using items directly from (Hong and Cha 2013).

In each of the online surveys, the items for the dependent variable, PBOS, were presented on a screen immediately after the subjects were shown a sample email sent from a prominent bank (name disguised) to its customers right after the Target data breach of 2013. The e-mail alerted customers of the bank about the Target breach and that the bank was monitoring customer accounts for suspicious activity. Respondents were asked to answer the PBOS items keeping this incident and a retail chain/store in mind that operates like Target (i.e. allows shopping both through a website as well as through physical stores). Right after the survey items, the respondents were asked to verify which website they had in mind when responding to the PBOS items. We called this item TAR. As will be shown in the results of our PLS analysis later, controlling for TAR showed that a significant difference in the scores for our dependent variable for both the datasets.

Majority of the senior citizens respondents were in the 65-69 years age-group (27%) while in terms of gender the dataset was evenly split (51% females). Among the younger group, majority of the responses came from the range 18-30 year olds (40%) with gender equally split there as well. All respondents had engaged in online shopping at least once in their life. While a few of the younger subjects (13%) had not heard of the Target data breach (others had, thanks to the media coverage), only 5 out of 205 senior citizens respondents were not aware of this incident. That was reflected in the fact that 32.7% of the younger subjects and 47.8% of the senior citizens subjects confirmed that they had assumed Target as an example store when responding to items measuring PBOS.

We found that 29% of the younger and 24% of the senior citizens subjects had shopped at a website that at least once faced a hacking incident. Among the younger subjects, 13% had fallen victim to Internet scams in general and 14% were victims of some form of identity theft. The numbers on the senior citizens side were a little on the higher side (i.e. 19% and 17%,

respectively). The difference between these two broad age groups in terms of computer courses and workshops taken was slightly different. 45% of the younger population had participated in such courses while for the senior citizens, that number was 39%.

5. Analysis and Results

The research model (Figure 1) proposed earlier is evaluated using Partial Least Squares (PLS) (Chin 1998). This method has been shown to be robust to reasonable sample sizes (Cassel et al. 1999) and lack of normality for most variables in a dataset (Chin et al. 2003). PLS regression is conducted on the two groups of survey-generated datasets (young and senior citizens) using SmartPLS (Ringle et al. 2005), a tool that has been widely adopted by both Information Systems (Marcoulides et al. 2009; Ringle et al. 2012) and Marketing (Hair et al. 2012) researchers. For each variable in the path model, we chose a reflective measurement model (Coltman et al. 2008; Götz et al. 2010). Table 4 in Appendix A presents survey items what we used for our path model. In addition, as seen in the tables (table 5 and table 6) in Appendix B, both analyses resulted in satisfactory quality criteria (i.e., AVE, Communality, Composite Reliability and Chronbach's Alpha) (Hair et al. 2011). In addition, the output in both cases satisfied the Fornell-Larcker condition (Fornell and Larcker 1981) demonstrating the discriminant validity of our survey instrument. While the overall quality of both the models was satisfactory, the path coefficients and the R^2 values of the endogenous variables were found to be quite different. The path coefficients of the PLS analysis for both the models along with their significances are given in a table 2 below. The same has been depicted on the path analysis diagrams in Appendix B. (Figure 2 and Figure 3)

In the third last row of table 2, we have included the path coefficient from a variable called TAR to our dependent variable PBOS. In the PLS analysis with both the datasets, we found a statistically significant negative influence of TAR on PBOS. TAR is an indicator variable confirming if the respondent kept Target in mind when responding to the questions measuring

Data Breaches and Online Shopping

PBOS. This was a way of verifying that the sample email from the bank was a reminder of the Target data breach that was strong enough to influence the respondent to think about her current shopping activities with respect to Target. We found, as the table and the diagrams in Appendix B show that for both age groups, there would be a significant reconsideration taking place in the minds of the respondents had they placed themselves in the shoes of a Target customer. This finding perhaps shows the effect of empathy on shopping intent. We used the following controls: education level (measured on a 1-4 level, with 1 being high school), gender and assumed target.

Table 2: Results from SmartPLS

Senior citizens (>=55)					Younger (<55)				
Hypotheses		R^2			R^2		Hypotheses		
H1(-): PS -> PBOS	-0.168*	PBOS	0.390		PBOS	0.181	-0.185^	H1(-): PS -> PBOS	
H2(-): MON -> H1(-)	-0.215*						-0.036	H2(-): MON -> H1(-)	
H3(-): POSR -> PBOS	-0.100^						0.064	H3(-): POSR -> PBOS	
H4(+): PS -> POSR	0.201*	EA	0.243		EA	0.178	0.405***	H4(+): PS -> POSR	
H5(+): EA -> PBOS	0.333***						0.246*	H5(+): EA -> PBOS	
H6(-): POSR -> EA	-0.146*						-0.159*	H6(-): POSR -> EA	
H7(+): TBSS -> EA	0.441***	POSR	0.040		POSR	0.164	0.372***	H7(+): TBSS -> EA	
H8(+): TBSS -> PBOS	0.151*						0.137^	H8(+): TBSS -> PBOS	
TAR -> PBOS	-0.181*						-0.144*	TAR -> PBOS	
EDU -> PBOS	-0.013						-0.042	EDU -> PBOS	
GEN -> PBOS	0.164*						-0.007	GEN -> PBOS	

^ $p < 0.10$, * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

PS: Perceived Severity, MON: Internal Monitoring, POSR: Perceived Online Shopping Risk, PBOS: Post-Breach Online Shopping, EA: E-Commerce Attitude, TBSS: Trusting Beliefs in Shopping Services, TAR: Assumed Target, EDU: Education, GEN: Gender

We analyzed the model with respect to each age-group (i.e. below-55 against above-55) in our research model. This effect was examined using multigroup analysis in PLS (Chin 2000;

Keil et al. 2000). This method performs a t-test between the pair of corresponding path coefficients for the groups. For example, the coefficients of the path representing hypothesis 1 (PS → PBOS, Table 2) for the older and the younger adults were used in a t-test. The t-value and its corresponding p-value indicate the statistical significance of the difference between the two path coefficients. The formula (Chin 2000) for computing this t-value is as follows:

$$t = \frac{Path_{sample1} - Path_{sample2}}{\sqrt{\frac{(m-1)^2}{(m+n-2)} \cdot s.e.^2_{sample1} + \frac{(n-1)^2}{(m+n-2)} \cdot s.e.^2_{sample2} \cdot \sqrt{\frac{1}{m} + \frac{1}{n}}}} \sim t_{m+n-2}$$

where m is the sample size of sample 1 (i.e. older adults) and n is the sample size of sample 2 (i.e. younger adults). The t-value thus computed has a degree of freedom $m + n - 2$. “s.e.” refers to the standard error for the particular path under consideration in each sample. These values are obtained from the re-sampling procedure called bootstrapping implemented in SmartPLS which gives the standard error for each path. Based on the datasets obtained through our online survey, Table 3 show the outcome of the pairwise multigroup analysis of our research model between senior citizens and younger adults.

Table 3: Multigroup Analysis between Senior Citizens and Younger Adults

	Path	t-statistic	2-sided p-value	Significance
H1	PS → PBOS	0.310	0.757	NS
H2	MON → (PS → PBOS)	0.841	0.401	NS
H3	POSR → PBOS	2.103	0.036	5%
H4	PS → POSR	1.505	0.133	NS
H5	EA → PBOS	0.617	0.538	NS
H6	POSR → EA	0.161	0.872	NS
H7	TBSS → EA	0.446	0.656	NS
H8	TBSS → PBOS	0.015	0.988	NS
	TAR → PBOS	0.340	0.734	NS
	EDU → PBOS	0.230	0.818	NS
	GED → PBOS	2.275	0.024	5%

NS: Not Significant, PS: Perceived Severity, MON: Internal Monitoring, POSR: Perceived Online Shopping Risk, PBOS: Post-Breach Online Shopping, EA: E-Commerce Attitude,

TBSS: Trusting Beliefs in Shopping Services, TAR: Assumed Target, EDU: Education, GEN: Gender

The results in Table 3 show that the two populations are distinct in some ways. Significant differences between the two populations pertain to perceived online shopping risk (POSR). This implies that someone who is fearful of risks associated with online shopping is more affected by actual incidents. Thus, it appears that younger adults who have generally been less worried about risks may have decided to engage in online shopping for other reasons than older adults. Perceived severity and risk are thus more important drivers of online shopping behavior after incidents for the older generations. The path coefficient is larger (in absolute value) for senior citizens for H3 (POSR $\rightarrow$ PBOS). In addition, the effect of gender was significantly different on post breach online shopping behavior between two groups. For younger adult groups, gender did not show any statistically significant difference on PBOS. However, for the senior citizen group, gender showed significant results. Especially, on average (for older adults), female group has 0.164 higher PBOS than male group.

6. Discussion

In this section we discuss the findings, the rejection of certain hypothesis in both age groups and the dissimilarity in significance of path coefficients between the two. To summarize, the results tell us that the research model we proposed explains an older adult user's response to Target and other breaches much better than it does for people below the age of 55.

One of the key areas where younger people differed from their older counterparts is the rejection of hypothesis H2. This hypothesis implies that monitoring habit negatively influences effect of perceived severity on shopping intent after being reminded about the Target incident. As per our discussions earlier, monitoring, measured by regularity of keeping an eye on bank statements, is an indicator of security consciousness that is supposed to mitigate the feeling of threat and uncertainty. The latter arises not only when a shopping website cannot be transparent

Data Breaches and Online Shopping

about the shopping experience, but also when news of data breaches in retail chains is floating around. It appears from the PLS output that security consciousness or simply monitoring (MON) cannot temper this fear in younger people. We can speculate here that this is an indicator, in turn, of their awareness of the relative lack of usefulness of monitoring in trying to actually curb threats. In other words, monitoring can give one person a mental satisfaction but people familiar with the workings of shopping and the Web in general may realize that breaches are often inevitable or not easily stoppable.

Prior literature (Cho 2006; McKnight and Choudhury 2006) has demonstrated the negative impact of perceived risks to security, privacy and service on intentions related to online shopping. This negative impact is significant amongst the older generations as opposed to their younger counterparts. To understand this difference, we need to draw attention to the actual construct being evaluated here as a dependent variable. PBOS intent is measured in the context of a massive data breach and in the light of its potential impact on Target customers whereby a bank had to send out mass email alerts. This knowledge can very well orient the thought process of a respondent towards a more risk-averse position regarding online shopping. We did not see significant negative effect of the perceived risk on the dependent variable for young adults. However, this was significant for the older generations.

The final aspect where the output from the two samples differed was the impact of trusting beliefs of shopping services (TBSS) on PBOS. In traditional trust literature this relationship is well known. However, our data shows that when the end result is a behavior in the aftermath of a security threat, this relationship may not hold especially with a modern Internet-savvy population. A high level of trust in the shopping service offered by a website does not automatically translate to intended purchase and other shopping-related activities especially with sites that resemble Target.com, now that so many data breaches have come to the public's knowledge. The finding from the analysis with the senior citizens dataset indicates the opposite –

Data Breaches and Online Shopping

i.e. senior citizens treat shopping service and security aspects separately. This difference between the two age categories deserves further investigation.

The practical implication of this study lies in its application in policy-making. One of the findings from our survey is that perceived online shopping risk is a stronger determinant of post-breach shopping intentions in older adults. This implies that in the event of any large scale data breach at a popular organization, one of the tasks to undertake is for breached organizations to convince their older clientele about the security measures that can prevent any such future breach. Such steps would help ensure continued business and transactions from this demography. The importance of internal monitoring also implies that e-commerce organizations can benefit by promoting campaigns about the value of staying alert about online transactions. The increased practice of doing so in the form of checking bank statements would again help ensure continued engagement even after a breach has occurred. This would presumably be more than likely to be true with senior citizens. In addition, for the relationship between PS and PBOS, we found significant effect for older adults and marginally significant effects for young adults groups. That means the customers' perception of severity (PS) is significant when it comes to their likelihood to continue online shopping even after a data breach. The result of younger adult groups is interesting. We hypothesized that PS had a negative impact on PBOS. Readers would be somewhat surprised to see this finding that perceived severity of younger adults group is only marginally significant on PBOS. Our recommendations and implications could apply more directly to online shopping and retail organizations that happen to have a brick-and mortar presence.

7. Conclusion

This study has a few limitations, one being that we were not able to conduct a longitudinal study whereby we could have tested the online shopping intent (PBOS) both before and after a certain data breach. While it is not possible to anticipate a particular data breach

Data Breaches and Online Shopping

incident, these incidents keep happening often. A longitudinal study is thus indeed possible where a post-event survey would be conducted as soon as a breach has been announced on some of the media outlets. A pre-post study would also be possible to be conducted entirely after the breach if we can select appropriate samples to control for the awareness of a certain breach. This was not possible with something as mainstream as the Target breach.

Further, we have divided the entire population into two broad age-based categories. This type of grouping glosses over the uniqueness that may be associated within certain age-based cohorts. While we have theorized our model from an age perspective (senior citizens against others), that is still too broad given that not every cohort within either category were introduced to computers and the Internet at the same time. However, this richness can be elicited only from a much larger sample that can guarantee sufficient power within each age-cohort and this was something that could not have been achieved at this time due to resource constraints. One more aspect about sampling that limits our study is that we did not ensure to pick both Target and non-Target customers in equal measures in order to control for the personal stake in the fallout from the data breach at that chain. This objective is difficult to fulfil as we cannot anticipate which store's website will be breached.

Other limitations include not considering income or socio-economic status of our subjects for the model. Before making a decision about online shopping, a customer may do a cost-benefit analysis. This analysis may differ from person to person depending on her economic status and on the price and value of the product(s). We plan to test this aspect in a future study. Internal monitoring in our study is essentially the frequency of keeping track of charges. This requires a cognitive burden and in the survey, we have not asked questions that elicit such burdens. The lack of constructs and items measuring the extent and nature of online shopping is a limitation in our study. Including such items, however, would have increased the length of our survey questionnaire. Long questionnaires have been shown to evoke less thoughtful responses.

To summarize, in this paper, we have presented a very topical investigation of attitude and intentions about online shopping activities under the awareness of recent large-scale data breaches at major retail stores like Target and Neiman Marcus. While privacy and security concerns have been historically studied as some of the key antecedents to the adoption of online shopping, in a 21st century environment that adoption has almost crossed the tipping point. It is thus now important to understand how the adoption will change given the spate of attacks that online properties around the world are facing from organized and individual cybercriminals. Our investigation has practical implications due to its focus on the generational difference in perception of these modern security risks and how they are channeled towards altering shopping-related decisions. By incorporating personal actions like bank account monitoring, though limited in its usefulness, we have put forward a richer understanding of the security and privacy focus in the online shopping context. Our research model was built on top of extant literature and pieced together from fundamental theories about trust, risk. This model has been validated using data collected from an online survey and the striking differences observed between the senior citizens generation and the rest of the U.S. population should serve as a foundation for further age-based technology adoption research.

9. Acknowledgement

The authors would like to thank the SE and review team for critical comments that have greatly improved the paper. This research was funded by the National Science Foundation (NSF) under Grant 0916612 and 1227353. We would like to thank Md Shamim Akbar for research assistance. The usual disclaimer applies.

References:

- Acquisti, A., and Grossklags, J. 2005. "Privacy and Rationality in Individual Decision Making," *IEEE Security & Privacy* (2), pp. 24-30.
- Aksoy, L., van Riel, A., Kandampully, J., Bolton, R. N., Parasuraman, A., Hoefnagels, A., Migchels, N., Kabadayi, S., Gruber, T., and Komarova Loureiro, Y. 2013. "Understanding Generation Y and Their Use of Social Media: A Review and Research Agenda," *Journal of Service Management* (24:3), pp. 245-267.
- Alreck, P. L., DiBartolo, G. R., Diriker, M., Dover, H. F., Passyn, K. A., and Settle, R. B. 2011. "Time Pressure, Time Saving and Online Shopping: Exploring a Contradiction," *Journal of Applied Business Research (JABR)* (25:5).
- Baier, A. 1995. *Moral Prejudices: Essays on Ethics*. Harvard University Press.
- Banjo, S. a. F., D. 2014. "Stores Confront New World of Reduced Shopper Traffic," in: *The Wall Street Journal*.
- Bauer, R. A. 1960. "Consumer Behavior as Risk Taking," *Dynamic marketing for a changing world* (398).
- Belanger, F., Hiller, J. S., and Smith, W. J. 2002. "Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes," *The Journal of Strategic Information Systems* (11:3), pp. 245-270.
- Bhatnagar, A., Misra, S., and Rao, H. R. 2000. "On Risk, Convenience, and Internet Shopping Behavior," *Commun. ACM* (43:11), pp. 98-105.
- Buffett, S., Fleming, M., Richter, M., Scott, N., and Spencer, B. 2004. "Determining Internet Users' Values for Private Information,").
- Cassel, C., Hackl, P., and Westlund, A. H. 1999. "Robustness of Partial Least-Squares Method for Estimating Latent Variable Quality Structures," *Journal of applied statistics* (26:4), pp. 435-446.
- Chang, E.-C., and Tseng, Y.-F. 2013. "Research Note: E-Store Image, Perceived Value and Perceived Risk," *Journal of Business Research* (66:7), pp. 864-870.
- Childers, T. L., Carr, C. L., Peck, J., and Carson, S. 2002. "Hedonic and Utilitarian Motivations for Online Retail Shopping Behavior," *Journal of retailing* (77:4), pp. 511-535.
- Chin, W. W. 1998. "The Partial Least Squares Approach to Structural Equation Modeling," *Modern methods for business research* (295:2), pp. 295-336.
- Chin, W. W. 2000. "Frequently Asked Questions – Partial Least Squares and Pls-Graph." Retrieved September 2, 2014, from <http://disc-nt.cba.uh.edu/chin/plsfaq.htm>
- Chin, W. W., Marcolin, B. L., and Newsted, P. R. 2003. "A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic-Mail Emotion/Adoption Study," *Information systems research* (14:2), pp. 189-217.
- Chiu, C. M., Wang, E. T., Fang, Y. H., and Huang, H. Y. 2014. "Understanding Customers' Repeat Purchase Intentions in B2c E-Commerce: The Roles of Utilitarian Value, Hedonic Value and Perceived Risk," *Information Systems Journal* (24:1), pp. 85-114.
- Cho, J. 2006. "The Mechanism of Trust and Distrust Formation and Their Relational Outcomes," *Journal of retailing* (82:1), pp. 25-35.
- Clearinghouse, P. R. 2012. from <http://www.privacyrights.org/data-breach/new>

- CMO. 2014. "15 Mind-Blowing Stats About Online Shopping." from http://www.cmo.com/articles/2014/5/6/Mind_Blowing_Stats_Online_Shopping.html
- Coltman, T., Devinney, T. M., Midgley, D. F., and Venaik, S. 2008. "Formative Versus Reflective Measurement Models: Two Applications of Formative Measurement," *Journal of Business Research* (61:12), pp. 1250-1262.
- Dark_Reading. 2010. "Itrc Study: Loss of Credit Card Information and Merchant Data Breach Cited as Priority Concerns to Consumers." Retrieved 10/10, 2015, from <http://www.darkreading.com/risk/itrc-study-loss-of-credit-card-information-and-merchant-data-breach-cited-as-priority-concerns-to-consumers/d/d-id/1134204?>
- Davis, F. D. 1989. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS quarterly*), pp. 319-340.
- Doolin, B., Dillon, S., Thompson, F., and Corner, J. L. 2005. "Perceived Risk, the Internet Shopping Experience and Online Purchasing Behavior: A New Zealand Perspective," *Journal of Global Information Management* (13:2), pp. 66-88.
- Featherman, M. S., Miyazaki, A. D., and Sprott, D. E. 2010. "Reducing Online Privacy Risk to Facilitate E-Service Adoption: The Influence of Perceived Ease of Use and Corporate Credibility," *Journal of Services Marketing* (24:3), pp. 219-229.
- Forbes. 2014. "Data Breach Bulletin: Brazilian Banks Lose \$3.75 Billion Because of Boleto Malware." from <http://www.forbes.com/sites/katevinton/2014/07/07/data-breach-bulletin-brazilian-banks-lose-3-75-billion-because-of-boleto-malware/>
- Fornell, C., and Larcker, D. F. 1981. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of marketing research*), pp. 39-50.
- Goldfarb, A., and Tucker, C. 2012. "Shifts in Privacy Concerns," *The American Economic Review* (102:3), pp. 349-353.
- Götz, O., Liehr-Gobbers, K., and Krafft, M. 2010. "Evaluation of Structural Equation Models Using the Partial Least Squares (PLS) Approach," in *Handbook of Partial Least Squares*. Springer, pp. 691-711.
- Grabner-Kraeuter, S. 2002. "The Role of Consumers' Trust in Online-Shopping," *Journal of Business Ethics* (39:1-2), pp. 43-50.
- Grimes, G. A., Hough, M. G., Mazur, E., and Signorella, M. L. 2010. "Older Adults' Knowledge of Internet Hazards," *Educational Gerontology* (36:3), pp. 173-192.
- Hair, J. F., Ringle, C. M., and Sarstedt, M. 2011. "PLS-Sem: Indeed a Silver Bullet," *The Journal of Marketing Theory and Practice* (19:2), pp. 139-152.
- Hair, J. F., Sarstedt, M., Ringle, C. M., and Mena, J. A. 2012. "An Assessment of the Use of Partial Least Squares Structural Equation Modeling in Marketing Research," *Journal of the Academy of Marketing Science* (40:3), pp. 414-433.
- Hoffman, D. L., Novak, T. P., and Peralta, M. 1999. "Building Consumer Trust Online," *Communications of the ACM* (42:4), pp. 80-85.
- Hong, I. B., and Cha, H. S. 2013. "The Mediating Role of Consumer Trust in an Online Merchant in Predicting Purchase Intention," *International Journal of Information Management* (33:6), pp. 927-939.
- Ives, B., Walsh, K. R., and Schneider, H. 2004. "The Domino Effect of Password Reuse," *Communications of the ACM* (47:4), pp. 75-78.

- Keil, M., Tan, B. C., Wei, K.-K., Saarinen, T., Tuunainen, V., and Wassenaar, A. 2000. "A Cross-Cultural Study on Escalation of Commitment Behavior in Software Projects," *Mis Quarterly*, pp. 299-325.
- Khalifa, M., and Limayem, M. 2003. "Drivers of Internet Shopping," *Communications of the ACM* (46:12), pp. 233-239.
- Kumar, A., and Lim, H. 2008. "Age Differences in Mobile Service Perceptions: Comparison of Generation Y and Baby Boomers," *Journal of Services Marketing* (22:7), pp. 568-577.
- Lee, G.-G., and Lin, H.-F. 2005. "Customer Perceptions of E-Service Quality in Online Shopping," *International Journal of Retail & Distribution Management* (33:2), pp. 161-176.
- Lee, J., Lee, J.-N., and Tan, B. C. 2012. "Antecedents of Cognitive Trust and Affective Distrust and Their Mediating Roles in Building Customer Loyalty," *Information Systems Frontiers*, pp. 1-17.
- Lee, M., and Lee, J. 2012. "The Impact of Information Security Failure on Customer Behaviors: A Study on a Large-Scale Hacking Incident on the Internet," *Information Systems Frontiers* (14:2), pp. 375-393.
- Ling, K. C., Chai, L. T., and Piew, T. H. 2010. "The Effects of Shopping Orientations, Online Trust and Prior Online Purchase Experience toward Customers' Online Purchase Intention," *International Business Research* (3:3), p. p63.
- Luhmann, N. 1979. "Trust and Power. 1979," *John Willey & Sons*).
- Marcoulides, G. A., Chin, W., and Saunders, C. 2009. "Foreword: A Critical Look at Partial Least Squares Modeling," *Management Information Systems Quarterly* (33:1), p. 10.
- McKnight, D. H., and Chervany, N. 2001. "Trust and Distrust Definitions: One Bite at a Time," *Trust in Cyber-societies*, pp. 27-54.
- McKnight, D. H., and Choudhury, V. 2006. "Distrust and Trust in B2c E-Commerce: Do They Differ?," *ACM*, pp. 482-491.
- McKnight, D. H., Choudhury, V., and Kacmar, C. 2002. "Developing and Validating Trust Measures for E-Commerce: An Integrative Typology," *Information Systems Research* (13:3), pp. 334-359.
- Milne, G. R. 2003. "How Well Do Consumers Protect Themselves from Identity Theft?," *Journal of Consumer Affairs* (37:2), pp. 388-402.
- Mitzner, T. L., Boron, J. B., Fausset, C. B., Adams, A. E., Charness, N., Czaja, S. J., Dijkstra, K., Fisk, A. D., Rogers, W. A., and Sharit, J. 2010. "Older Adults Talk Technology: Technology Usage and Attitudes," *Computers in Human Behavior* (26:6), pp. 1710-1721.
- Miyazaki, A. D., and Fernandez, A. 2001. "Consumer Perceptions of Privacy and Security Risks for Online Shopping," *Journal of Consumer Affairs* (35:1), pp. 27-44.
- Morris, M. G., and Venkatesh, V. 2000. "Age Differences in Technology Adoption Decisions: Implications for a Changing Work Force," *Personnel psychology* (53:2), pp. 375-403.
- Moshrefjavadi, M. H., Dolatabadi, H. R., Nourbakhsh, M., Poursaeedi, A., and Asadollahi, A. 2012. "An Analysis of Factors Affecting on Online Shopping

- Behavior of Consumers," *International Journal of Marketing Studies* (4:5), p. p81.
- Nanji, A. 2013. "Online Shopping Trends 2013: Most Popular Categories, Top Purchase Drivers." *MarketingProfs*, from <http://www.marketingprofs.com/charts/2013/12195/online-shopping-trends-most-popular-categories-top-purchase-drivers>
- Nepomuceno, M. V., Laroche, M., and Richard, M.-O. 2014. "How to Reduce Perceived Risk When Buying Online: The Interactions between Intangibility, Product Knowledge, Brand Familiarity, Privacy and Security Concerns," *Journal of Retailing and Consumer Services* (21:4), pp. 619-629.
- Ng, B. Y., Kankanhalli, A., and Xu, Y. C. 2009. "Studying Users' Computer Security Behavior: A Health Belief Perspective," *Decision Support Systems* (46:4), pp. 815-825.
- Omodei, M. M., and McLennan, J. 2000. "Conceptualizing and Measuring Global Interpersonal Mistrust-Trust," *The journal of social psychology* (140:3), pp. 279-294.
- Peretti, K. K. 2008. "Data Breaches: What the Underground World of Carding Reveals," *Santa Clara Computer & High Tech. LJ* (25), p. 375.
- Piquero, N. L., Cohen, M. A., and Piquero, A. R. 2011. "How Much Is the Public Willing to Pay to Be Protected from Identity Theft?," *Justice Quarterly* (28:3), pp. 437-459.
- Reisenwitz, T., and Iyer, R. 2007. "A Comparison of Younger and Older Baby Boomers: Investigating the Viability of Cohort Segmentation," *Journal of Consumer Marketing* (24:4), pp. 202-213.
- Retailer, I. 2014. "How Consumers Pay Online." from <http://www.internetretailer.com/trends/consumers/>
- Ringle, C. M., Sarstedt, M., and Straub, D. W. 2012. "Editor's Comments: A Critical Look at the Use of Pls-Sem in *MIS Quarterly*," *MIS quarterly* (36:1), pp. iii-xiv.
- Ringle, C. M., Wende, S., and Will, A. 2005. "Smartpls 2.0 (Beta)." Hamburg, Germany.
- Roalf, D. R., Mitchell, S. H., Harbaugh, W. T., and Janowsky, J. S. 2011. "Risk, Reward, and Economic Decision Making in Aging," *The Journals of Gerontology Series B: Psychological Sciences and Social Sciences*, p. gbr099.
- Robinson, R. V., and Jackson, E. F. 2001. "Is Trust in Others Declining in America? An Age-Period-Cohort Analysis," *Social Science Research* (30:1), pp. 117-145.
- Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS quarterly* (35:4), pp. 989-1016.
- Soopramanien, D. G., and Robertson, A. 2007. "Adoption and Usage of Online Shopping: An Empirical Analysis of the Characteristics of "Buyers""Browsers"" and "Non-Internet Shoppers"," *Journal of Retailing and Consumer Services* (14:1), pp. 73-82.
- Sutter, M., and Kocher, M. G. 2007. "Trust and Trustworthiness across Different Age Groups," *Games and Economic Behavior* (59:2), pp. 364-382.
- Times, N. 2014. "Target Missed Signs of a Data Breach." from <http://www.nytimes.com/2014/03/14/business/target-missed-signs-of-a-data-breach.html>

Data Breaches and Online Shopping

- Verhagen, T., Vonkeman, C., Feldberg, F., and Verhagen, P. 2014. "Present It Like It Is Here: Creating Local Presence to Improve Online Product Experiences," *Computers in Human Behavior* (39), pp. 270-280.
- Vuori, S., and Holmlund-Rytkönen, M. 2005. "55+ People as Internet Users," *Marketing Intelligence & Planning* (23:1), pp. 58-76.
- Wang, T.-L., and Tseng, Y.-F. 2011. "A Study of the Effect on Trust and Attitude with Online Shopping," *International Journal of Digital Society* (2:2), pp. 433-440.
- Xu, H., Teo, H. H., and Tan, B. C. Y. 2005. "Predicting the Adoption of Location-Based Services: The Role of Trust and Perceived Privacy Risk."
- Zeller, T. 2005. "Black Market in Stolen Credit Card Data Thrives on Internet," *New York Times*).

Appendix A

Table 4: Survey Instrument

<i>Post-Breach Online Shopping (PBOS) (Hong & Cha 2013):</i>   PBOS1: I am likely to make another purchase from that website in the next year.   PBOS2: I intend to continue using that website rather than discontinue its use.   PBOS3: I will recommend that website to my friends.   PBOS4: I will recommend that website to my family.   PBOS5: I would reconsider saving any payment-related information on any shopping website in general.
<i>Internal Monitoring (IM):</i>   IM1. I track the charges on my bank statement..
<i>Perceived Severity (PS) (Ng et al. 2009):</i>   If a website where I do online shopping faced a hacking incident, it would...   PS1: ... be a serious problem for me.   PS2: ... have a negative effect on my shopping activities.   PS3: ... have a negative effect on my payment card (credit/debit) use.
<i>Perceived Online Shopping Risk (POSR) (Cho 2006):</i>   POSR1: Online shopping websites are vulnerable to hackers who may steal customers' information.   POSR2: Online shopping customers often face damaging and harmful behavior from hackers.   POSR3: Customers' information stored at online shopping websites is not safe.   POSR4: Customers are vulnerable in online shopping websites that had incidents of hacking.
<i>Trusting Beliefs in Shopping Services (TBSS) (Lee et al. 2012):</i>   TBSS1: I believe online shopping websites provide services as expected.   TBSS2: I have positive expectations regarding online shopping websites in their provisioning of shopping services   TBSS3: I am able to use online shopping services with confidence.
<i>E-Commerce Attitude (EA):</i>   I am comfortable _____ ...   EA1: ... shopping on the Internet.   EA2: ... saving credit/debit card information on a shopping website.   EA3: ... saving any personal information on a shopping website.
<i>Website Assumed (TAR):</i>   TAR1: Which shopping website did you have in mind when you answered the questions on the previous screen?

Appendix B – PLS Results:

PLS path model for data from young adults (<55)

(Sample size: 159)

^ $p < 0.10$, * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Figure 2: Path analysis result for young adults

PLS path model for data from senior citizens (≥ 55)

(Sample size: 205)

^ $p < 0.10$, * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Figure 3: Path analysis result for senior citizens

Table 5: PLS model overview for data from young adults (<55)

	AVE	Composite Reliability	Cronbach's Alpha	Communality
POSR	0.628191	0.871060	0.804686	0.628191
MON	1.000000	1.000000	1.000000	1.000000
EA	0.660752	0.853814	0.753090	0.660751
PBOS	0.741735	0.934877	0.913401	0.741735
PS	0.717978	0.883998	0.802111	0.717978
PS * MON	0.775660	0.911751	0.890022	0.775662
TAR	1.000000	1.000000	1.000000	1.000000
TBSS	0.617098	0.827235	0.704771	0.617098

Table 6: PLS model overview for data from senior citizens (>=55)

	AVE	Composite Reliability	Cronbach's Alpha	Communality
POSR	0.663836	0.944608	0.837023	0.663836
MON	1.000000	1.000000	1.000000	1.000000
EA	0.656210	0.851100	0.747802	0.656209
PBOS	0.741735	0.944608	0.926726	0.773296
PS	0.773296	0.898658	0.830632	0.747314
PS * MON	0.714017	0.881973	0.800875	0.714017
TAR	1.000000	1.000000	1.000000	1.000000
TBSS	0.740742	0.895368	0.826951	0.740742